WHITE PAPER

Secure Connectivity within HPE Azure Stack Hub Applications Using FortiGate VM, FortiManager, FortiAnalyzer, and FortiEDR

Introduction

For IT organizations supporting business transformation, the hybrid cloud offers an ideal solution for delivering the required service experience while maintaining control, ensuring performance, and assuring flexibility. A key element of a hybrid cloud solution is secure connectivity, which enables the seamless interworking of on-premises or third-party resources of the cloud computing environment with the public cloud. The security features of the connectivity option are key to ensuring that integrity of the hybrid cloud infrastructure as well as the data and applications it supports are well-protected.

Fortinet provides the complete visibility control all organizations need to secure their attack surface, keep up with ever increasing performance demands, and preserve the user experience across various cloud environments, including hybrid cloud. When employed with HPE ProLiant for Microsoft Azure Stack Hub, Fortinet helps offer a secure hybrid cloud environment as a full solution.

The HPE and Fortinet solution for Azure Hybrid Cloud combines the HPE ProLiant for Microsoft Azure Stack Hub with the FortiGate VM on Azure, FortiAnalyzer, FortiManager, and FortiEDR, to enable seamless and secure connectivity for hybrid cloud environments in multiple solution configurations jointly validated by HPE and Fortinet to ensure functionality and compatibility.

HPE ProLiant for Microsoft Azure Stack Hub

Microsoft created Microsoft Azure Stack Hub Hybrid Cloud as an on-premises extension of Azure Public Cloud, leveraging nearly identical services, tools, virtual infrastructure, and features. The value is the ability to easily transfer workloads across hybrid cloud and public cloud environments without the need for refactoring applications, virtual machines (VM), and services. Consistency is maintained for test and development; common portal interfaces reduce complexity and management, which greatly reduces total time from project start to finish.

One key challenge for hybrid cloud solutions is providing high availability to strategic workloads that must maintain constant availability due to regulatory compliance or data recovery requirements—all without adding additional complexity to the environment. HPE ProLiant for Microsoft Azure Stack Hub solution is a pre-engineered, pre-integrated, on-premises hybrid cloud solution jointly developed by Hewlett Packard Enterprise and Microsoft. It focuses on the ability to rapidly deploy a hybrid cloud environment that is fully compatible with Microsoft Azure Public Cloud. While customers modernize core business applications, HPE ProLiant for Microsoft Azure Stack Hub solution provides a single platform of resources that can be deployed as fully Azure Public Cloud ready. It enables quicker, more manageable resource deployment, allowing organizations to support data and applications, regardless of where the data lies, on-premises with Azure Stack Hub or in the Azure Public Cloud.

With the consistent infrastructure resources of the HPE ProLiant for Microsoft Azure Stack Hub solution, HPE and Fortinet have validated the FortiGate solutions for VNet peering and network security monitoring for applications running on Microsoft Azure Stack Hub environments. The FortiAnalyzer and FortiManager solutions protect access to and secure connectivity of tenant applications, including virtual machines.

HPE and Fortinet Enable Secure Connectivity, Network Monitoring, and Workload Protection for Microsoft Azure Stack Hub

HPE, working with Fortinet engineers, validated the functionality and compatibility of the FortiGate VM, FortiAnalyzer, FortiManager, and FortiEDR solution configurations for secure connectivity, network traffic control and monitoring, and workload protection. The validations were done to prove configurations with HPE ProLiant for Microsoft Azure Stack Hub, deployed as a hybrid cloud environment.

White Paper Goals

The goal of this white paper is to demonstrate the ability of Fortinet solutions along with HPE ProLiant for Microsoft Azure Stack Hub to:

- Successfully configure VNet peering for secure connectivity
- Monitor access and network traffic
- Successfully demonstrate traffic routing, monitoring reporting
- Offer workload infrastructure (VM) protection (with FortiEDR)

HPE Environment

Leveraging the Hewlett Packard Enterprise Azure Stack Innovation Center in Bellevue, Washington, validation tests were performed for complete solution sets. HPE is one of the few OEM vendors with dedicated centers to conduct Microsoft Azure Stack Hub meetings, demos, and proof-of-concept (POC) activities with multiple locations worldwide.

HPE deployed the HPE ProLiant for Microsoft Azure Stack Hub environment for testing as described in Figure 1.

The validation environment utilized consisted of:

- 4-node Microsoft Azure Stack Hub instance deployed on HPE ProLiant DL380 Gen10 based configurations
- Fortinet FortiManager and FortiAnalyzers running as virtual appliances outside of Azure Stack Hub with local network connectivity

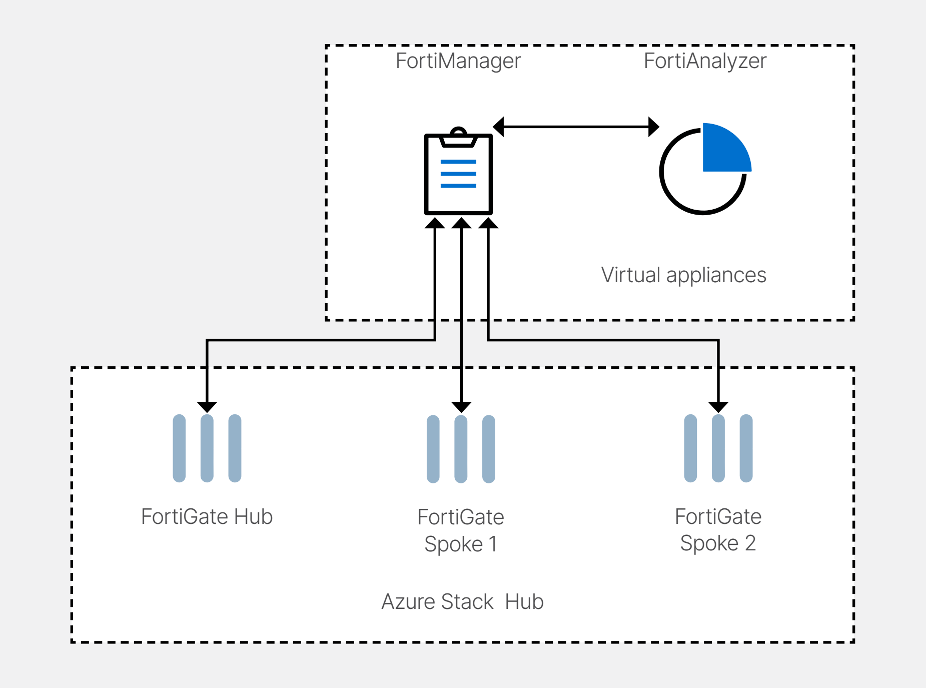


Figure 1: Fortinet virtual appliance configuration overview.

Validation test 1: VNet peering

A separate HPE DL360 jump host was used for accessing resources in Azure Stack subscription and testing connectivity.

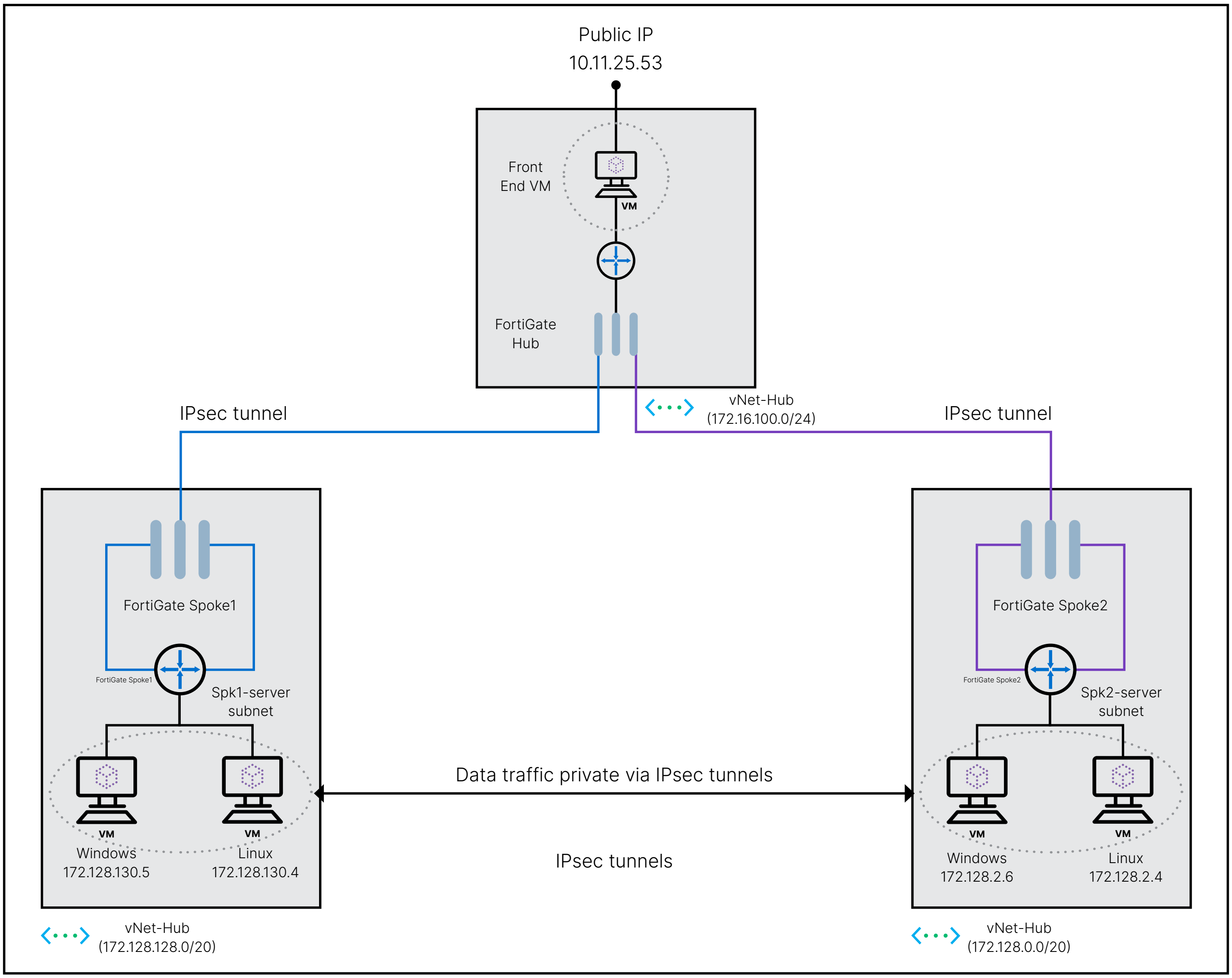
The example setup consists of three separate virtual networks within a user subscription in Azure Stack Hub. FortiGate VM was made available via the marketplace item syndication process within Azure Stack Hub.

Each virtual network consists of:

- Separate private IP address scope (for better clarification)
- Private network subnet for running Windows and Linux virtual machines used to test VNet-to-VNet connectivity
- FortiGate VM instance configured to virtual network's private subnets

Spoke1 and Spoke2 virtual networks contain Windows and Linux virtual machines to illustrate application workloads running in isolated, separate networks within Azure Stack Hub. A fully meshed IPSec tunnel configuration was deployed from FortiManager to allow Hub to Spokes, and Spoke to Spoke, intercommunication. VNet-to-VNet connectivity was confirmed from within Windows and Linux virtual machines from Spoke1 to Spoke2 and vice versa.

The Windows virtual machine in Hub virtual network was used to connect into the environment, similar to a jump host with access to application workload. This virtual machine was assigned a public IP from Azure Stack Hub for external connectivity.



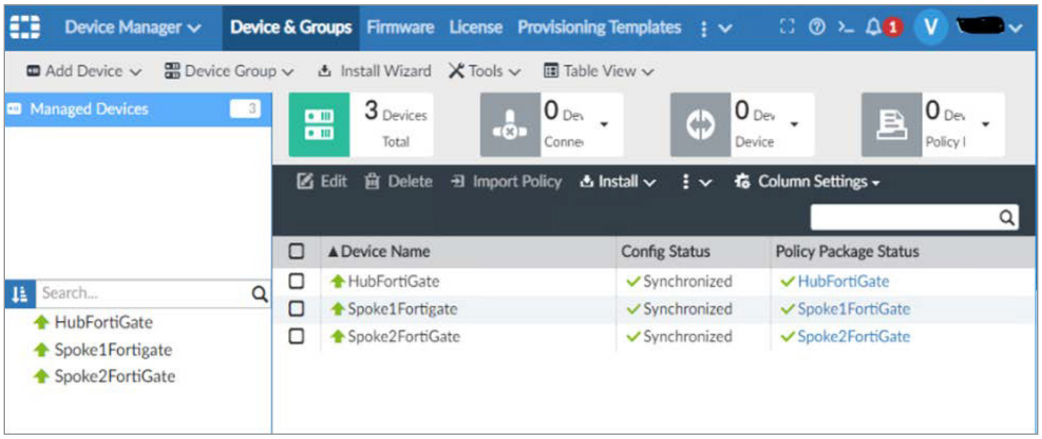
Azure Stack User Subscription

Figure 2: Virtual network with FortiGate configuration within Azure Stack Hub.

Validation test 2: Central management of VPN devices and IPsec connection monitoring

In the second validation test, FortiAnalyzer and FortiManager were configured to monitor all network traffic flowing through each FortiGate VM in Hub, Spoke1, and Spoke2 virtual networks.

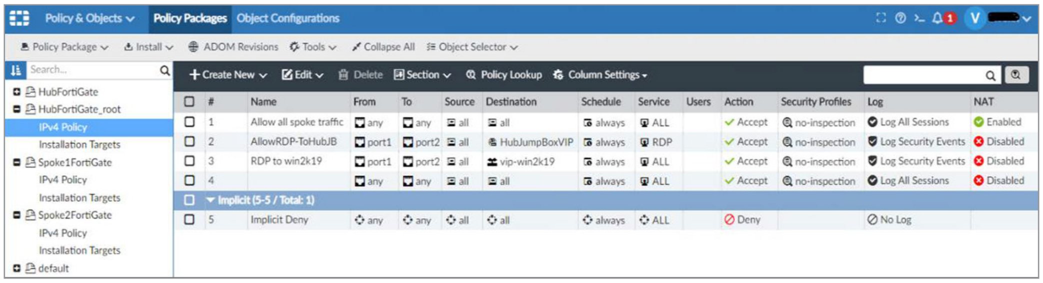
FortiManager was used to manage FortiGate instances in Hub, Spoke1, and Spoke2. The Policy & Objects feature within FortiManager was used to define device configurations specific to each FortiGate. FortiManager was also used to define and control IPsec tunnels from Hub to Spokes and Spoke to Spoke.



Device Name	Config Status	Policy Package Status
HubFortiGate	✓ Synchronized	✓ HubFortiGate
Spoke1Fortigate	✓ Synchronized	✓ Spoke1FortiGate
Spoke2FortiGate	✓ Synchronized	✓ Spoke2FortiGate

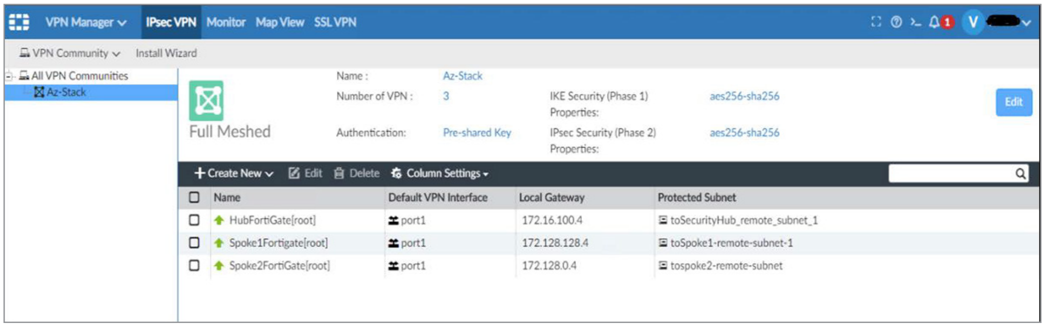
HubFortiGate
Spoke1Fortigate
Spoke2FortiGate

Figure 3: FortiGate Device Manager inventory within FortiManager.



#	Name	From	To	Source	Destination	Schedule	Service	Users	Action	Security Profiles	Log	NAT
1	Allow all spoke traffic	any	any	all	all	always	ALL		✓ Accept	no-inspection	Log All Sessions	Enabled
2	AllowRDP-ToHubJB	port1	port2	all	HubJumpBoxVIP	always	RDP		✓ Accept	no-inspection	Log Security Events	Disabled
3	RDP to win2k19	port1	port2	all	vip-win2k19	always	ALL		✓ Accept	no-inspection	Log Security Events	Disabled
4		any	any	all	all	always	ALL		✓ Accept	no-inspection	Log All Sessions	Disabled
Implicit (5-5 / Total: 1)												
5	Implicit Deny	any	any	all	all	always	ALL		Deny		No Log	

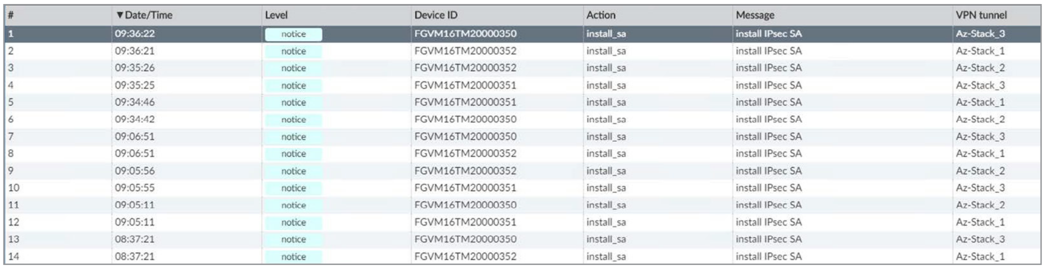
Figure 4: FortiGate policy packages within FortiManager.



Name : Az-Stack
Number of VPN : 3
Authentication: Pre-shared Key
IKE Security (Phase 1) Properties: aes256-sha256
IPsec Security (Phase 2) Properties: aes256-sha256

Name	Default VPN Interface	Local Gateway	Protected Subnet
HubFortiGate[root]	port1	172.16.100.4	toSecurityHub_remote_subnet_1
Spoke1Fortigate[root]	port1	172.128.128.4	toSpoke1-remote-subnet-1
Spoke2FortiGate[root]	port1	172.128.0.4	tospoke2-remote-subnet

Figure 5: FortiGate IPsec VPN Management within FortiManager.



#	▼Date/Time	Level	Device ID	Action	Message	VPN tunnel
1	09:36:22	notice	FGVM16TM20000350	install_sa	install IPsec SA	Az-Stack_3
2	09:36:21	notice	FGVM16TM20000352	install_sa	install IPsec SA	Az-Stack_1
3	09:35:26	notice	FGVM16TM20000352	install_sa	install IPsec SA	Az-Stack_2
4	09:35:25	notice	FGVM16TM20000351	install_sa	install IPsec SA	Az-Stack_3
5	09:34:46	notice	FGVM16TM20000351	install_sa	install IPsec SA	Az-Stack_1
6	09:34:42	notice	FGVM16TM20000350	install_sa	install IPsec SA	Az-Stack_2
7	09:06:51	notice	FGVM16TM20000350	install_sa	install IPsec SA	Az-Stack_3
8	09:06:51	notice	FGVM16TM20000352	install_sa	install IPsec SA	Az-Stack_1
9	09:05:56	notice	FGVM16TM20000352	install_sa	install IPsec SA	Az-Stack_2
10	09:05:55	notice	FGVM16TM20000351	install_sa	install IPsec SA	Az-Stack_3
11	09:05:11	notice	FGVM16TM20000350	install_sa	install IPsec SA	Az-Stack_2
12	09:05:11	notice	FGVM16TM20000351	install_sa	install IPsec SA	Az-Stack_1
13	08:37:21	notice	FGVM16TM20000350	install_sa	install IPsec SA	Az-Stack_3
14	08:37:21	notice	FGVM16TM20000352	install_sa	install IPsec SA	Az-Stack_1

Figure 6: IPsec VPN status logs within FortiAnalyzer.

Validation test 3: Workload infrastructure protection with FortiEDR

For the third validation test, we leveraged FortiEDR for next-generation, OS-agnostic endpoint protection for the Hub and Spoke workload servers. FortiEDR was able to provide protection from custom-built zero-day ransomware pre- and post-infection in real time. During our validation testing, FortiEDR prevented malware infection with its machine-learning antivirus and defused the potential threat while providing an automated response and remediation. Due to the low performance cost of FortiEDR, we were able to proactively reduce the attack surface of the workload server without sacrificing compute.

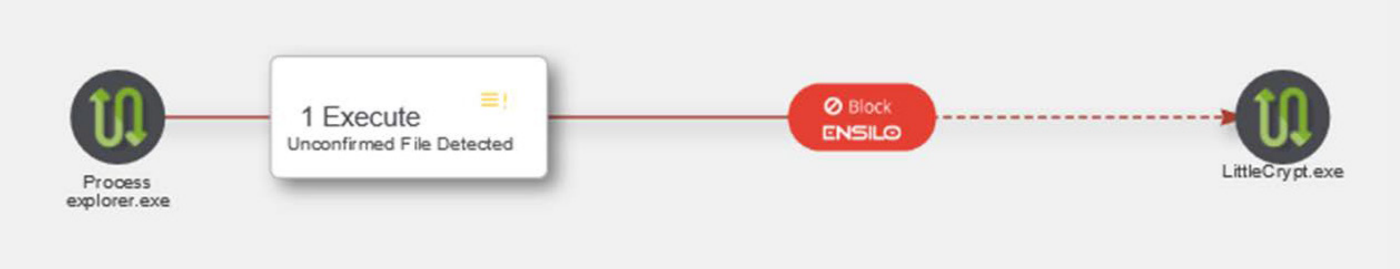


Figure 7: Real-time protection forensics within FortiEDR.

Real-time Fully Automated Security with Orchestrated Incident Response

How FortiEDR works

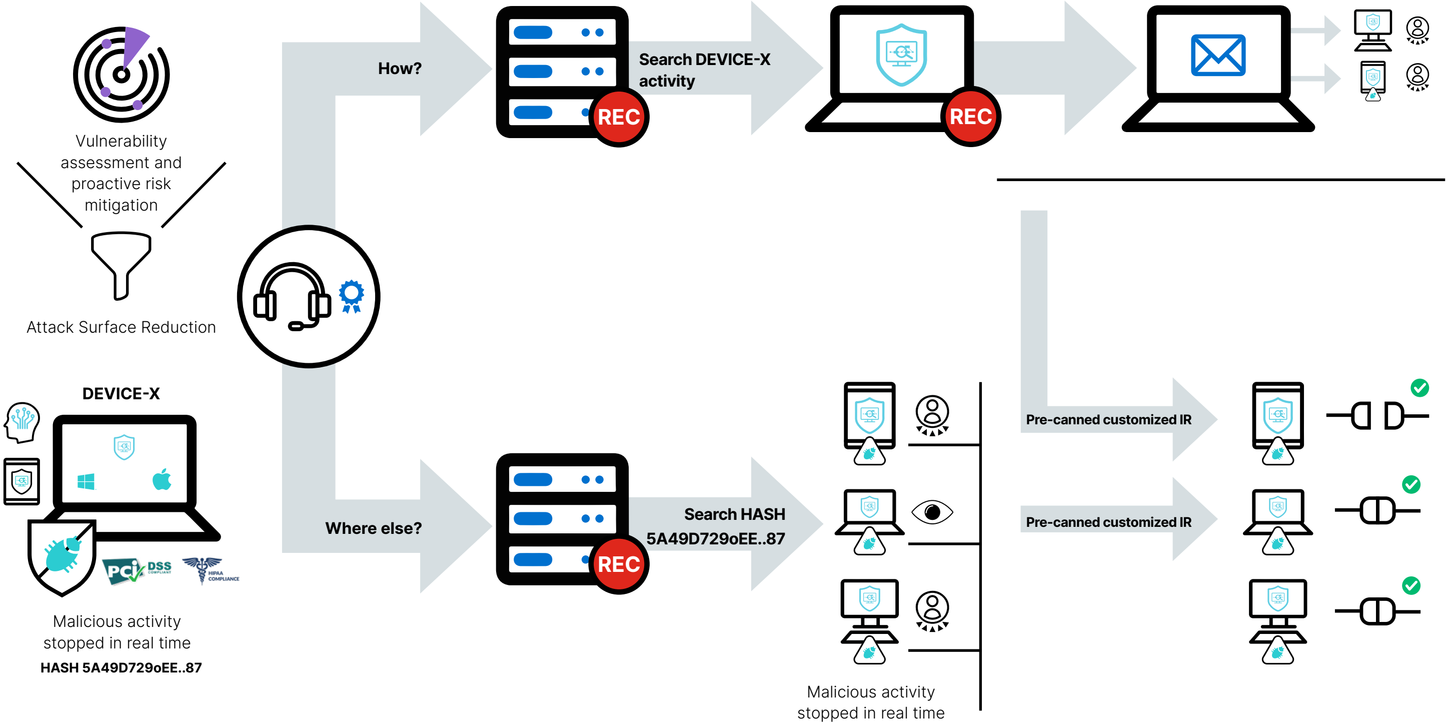

Vulnerability assessment and proactive risk mitigation
Attack Surface Reduction
DEVICE-X
Malicious activity stopped in real time
HASH 5A49D729oEE..87
How?
Search DEVICE-X activity
REC
REC
Where else?
REC
Search HASH 5A49D729oEE..87
Malicious activity stopped in real time
Pre-canned customized IR
Pre-canned customized IR

Figure 8: Conceptual overview of FortiEDR.

Summary

Fortinet delivers high-performance network security solutions that protect your network, users, and data from continually evolving threats. Fortinet's broad portfolio of top-rated solutions and centralized management enables security consolidation and delivers a simplified, end-to-end security infrastructure.

Combined with HPE's Azure Stack virtualization capabilities and solution offerings, security and compliance can be maintained while scaling to meet the needs of enterprise multi-tenant environments.

Partnership

Fortinet is a member of the HPE Partner Ready for Technology Partner program, an industry-leading approach to supply sophisticated integrated technologies in a simple, confident, and efficient manner. HPE is a member of the Fortinet Fabric-Ready Technology Alliance Partner Program, and part of the Fortinet Open Fabric Ecosystem, which provides integrated solutions to customers for comprehensive end-to-end security.

By participating in each other's programs, both HPE and Fortinet have access to the other's tools, processes, and resources to help our joint customers accelerate innovation and transformation that brings value, achieves business needs, and increases revenue and market share.

Additional Resources

Fortinet

- FortiGate VM
- FortiAnalyzer
- FortiManager
- FortiEDR
- HPE ProLiant for Microsoft Azure Stack Hub
- HPE Private Cloud Solutions

www.fortinet.com

May 12, 2021 8:50 AM

D:\Fortinet\2021 Rebranded templates\Marketing or Comms Request\April\Refresh\942802 - Alliance Refresh\wp-FA-secure-connectivity-within-hpe-azure-stack-5122021\wp-FA-secure-connectivity-within-hpe-azure-stack-5122021

985151-0-0-EN